

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 2.3
TÌM HIỂU VÀ CÀI ĐẶT, CẤU HÌNH MÁY CHỦ VPN**

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH.....	3
1.1 Mục đích.....	3
1.2 Tìm hiểu khái quát về VPN, các mô hình VPN và ứng dụng của VPN.....	3
1.2.1 VPN là gì?	3
1.2.2 Lợi ích và ưu điểm của VPN	3
1.2.3 VPN hoạt động như thế nào?	5
1.2.4 Các loại VPN	6
1.3 Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS.....	6
1.3.1 Giao thức đường hầm điểm-điểm PPTP (Point to Point Tunneling protocol)	7
1.3.2 Giao thức định hướng lớp 2 – L2F (Layer 2 Forwarding)	8
1.4 Các giao thức bảo mật cho VPN: IPSec, SSL/TLS.....	9
1.4.1 IPSec là gì?.....	9
1.4.2 Giao thức SSL/TLS	10
1.5 Tìm hiểu về SoftEther VPN	11
1.5.1 SoftEther VPN là gì?.....	11
CHƯƠNG 2. nội dung thực hành.....	12
2.1 Chuẩn bị môi trường	12
2.2 Các bước thực hiện.....	12
2.2.1 Chuẩn bị hệ thống	12
2.2.2 Cài đặt SoftEther VPN Server trên Linux	13
2.2.3 Cài đặt SoftEther VPN Client trên Windows.....	16
2.2.4 Tạo & kiểm tra kết nối VPN	16
KẾT LUẬN.....	19
TÀI LIỆU THAM KHẢO.....	19

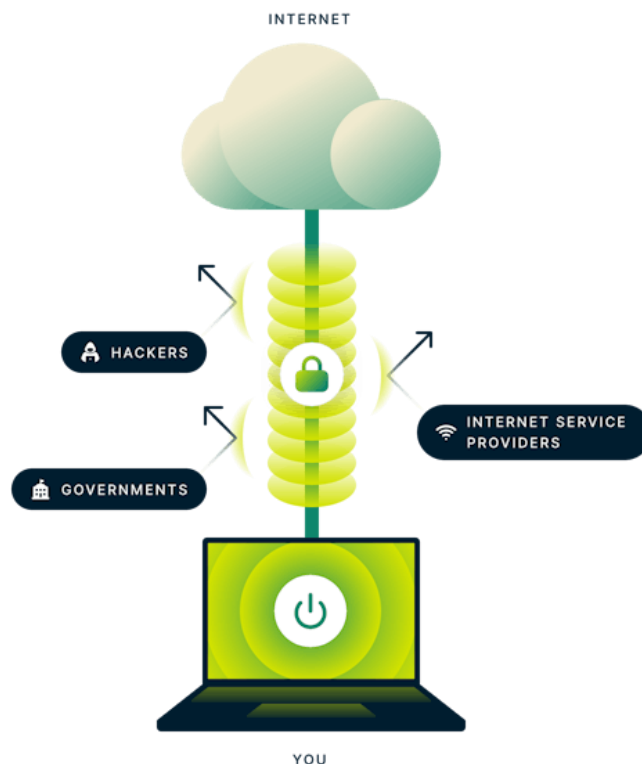
CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

- Tìm hiểu về mạng riêng ảo (VPN-Virtual Private Network), kiến trúc và hoạt động của mạng riêng ảo.
- Luyện tập kỹ năng cài đặt, cấu hình và vận hành máy chủ mạng riêng ảo (VPN server).

1.2 Tìm hiểu khái quát về VPN, các mô hình VPN và ứng dụng của VPN.

1.2.1 VPN là gì?



VPN hay mạng riêng ảo là đường hầm an toàn giữa thiết bị của bạn và internet. VPN bảo vệ bạn khỏi việc theo dõi, can thiệp và kiểm duyệt trực tuyến .

VPN (mạng riêng ảo) là cách dễ dàng và hiệu quả nhất để mọi người bảo vệ lưu lượng truy cập internet và giữ bí mật danh tính trực tuyến của họ. Khi bạn kết nối với máy chủ VPN an toàn, lưu lượng truy cập internet của bạn sẽ đi qua một đường hầm được mã hóa mà không ai có thể nhìn thấy , bao gồm cả tin tặc, chính phủ và nhà cung cấp dịch vụ internet của bạn.

Người tiêu dùng sử dụng VPN để giữ hoạt động trực tuyến của họ ở chế độ riêng tư và đảm bảo trải nghiệm internet của họ không bị can thiệp từ bên ngoài.

Các công ty sử dụng VPN để kết nối những nhân viên ở xa như thể họ đang sử dụng cùng một mạng cục bộ tại một văn phòng trung tâm, nhưng mang lại ít lợi ích hơn cho cá nhân so với VPN cá nhân.

1.2.2 Lợi ích và ưu điểm của VPN

- Thay đổi vị trí của bạn



Sử dụng VPN sẽ thay đổi địa chỉ IP của bạn , số duy nhất xác định bạn và vị trí của bạn trên thế giới. Địa chỉ IP mới này sẽ khiến bạn có vẻ như đang ở vị trí bạn chọn khi kết nối: Vương quốc Anh, Đức, Canada, Nhật Bản hoặc hầu như bất kỳ quốc gia nào, nếu dịch vụ VPN có máy chủ ở đó.

- Bảo vệ sự riêng tư của bạn



Thay đổi địa chỉ IP của bạn bằng VPN giúp bảo vệ danh tính của bạn khỏi các trang web, ứng dụng và dịch vụ muốn theo dõi bạn. Các VPN tốt cũng ngăn nhà cung cấp internet, nhà mạng di động và bất kỳ ai khác có thể đang nghe lén không nhìn thấy hoạt động của bạn, nhờ vào lớp mã hóa mạnh.

- Tăng cường bảo mật của bạn



Sử dụng VPN bảo vệ bạn khỏi các vi phạm bảo mật dưới nhiều hình thức, bao gồm đánh hơi gói tin, mạng Wi-Fi giả mạo và các cuộc tấn công trung gian. Khách du lịch, nhân viên làm việc từ xa và mọi loại cá nhân đang di chuyển đều sử dụng VPN bất cứ khi nào họ ở trên một mạng không đáng tin cậy như Wi-Fi công cộng miễn phí .

1.2.3 VPN hoạt động như thế nào?

1.2.3.1 Không có VPN

Khi bạn truy cập một trang web mà không có VPN, bạn đang được kết nối với trang web đó thông qua nhà cung cấp dịch vụ internet hoặc ISP của bạn. ISP sẽ chỉ định cho bạn một địa chỉ IP duy nhất có thể được sử dụng để nhận dạng bạn với trang web. Vì ISP của bạn đang xử lý và chỉ đạo tất cả lưu lượng truy cập của bạn, nên nó có thể biết được những trang web nào bạn truy cập. Và hoạt động của bạn có thể được liên kết với bạn bằng địa chỉ IP duy nhất đó.

1.2.3.2 Với VPN

Khi bạn kết nối internet bằng VPN, ứng dụng VPN trên thiết bị của bạn (còn gọi là máy khách VPN) sẽ thiết lập kết nối an toàn với máy chủ VPN . Lưu lượng truy cập của bạn vẫn đi qua ISP, nhưng ISP không còn có thể đọc hoặc thấy đích đến cuối cùng của lưu lượng truy cập đó nữa. Các trang web bạn truy cập không còn có thể thấy địa chỉ IP gốc của bạn nữa, mà chỉ có thể thấy địa chỉ IP của máy chủ VPN, được nhiều người dùng khác chia sẻ và thay đổi thường xuyên.

1.2.3.3 Cách thức hoạt động của VPN và những lợi ích mà nó mang lại

Ủy quyền:

- Máy chủ VPN hoạt động như một proxy hoặc máy chủ thay thế cho hoạt động web của bạn: Thay vì địa chỉ IP và vị trí thực của bạn, các trang web bạn truy cập sẽ chỉ thấy địa chỉ IP và vị trí của máy chủ VPN.
- Điều này giúp bạn ẩn danh hơn trên Internet.

Xác thực

- Việc thiết lập kết nối an toàn là một vấn đề khó khăn được giải quyết bằng thuật toán thông minh trong một quá trình gọi là xác thực .
- Sau khi xác thực, máy khách VPN và máy chủ VPN có thể chắc chắn rằng chúng đang nói chuyện với nhau chứ không phải với bất kỳ ai khác.

Đào hầm

- VPN cũng bảo vệ kết nối giữa máy khách và máy chủ bằng đường hầm và mã hóa.
- Đường hầm là một quá trình mà mỗi gói dữ liệu được đóng gói bên trong một gói dữ liệu khác. Điều này khiến bên thứ ba khó đọc hơn khi truyền dữ liệu.

Mã hóa

- Dữ liệu bên trong đường hầm cũng được mã hóa theo cách mà chỉ người nhận dự định mới có thể giải mã. Điều này giúp nội dung lưu lượng truy cập internet của bạn hoàn toàn riêng tư. Ngay cả nhà cung cấp dịch vụ internet của bạn cũng sẽ không nhìn thấy.

1.2.4 Các loại VPN

1.2.4.1 VPN thương mại

VPN thương mại, còn được gọi là VPN cá nhân hoặc VPN tiêu dùng, là dịch vụ riêng tư được cung cấp trực tiếp cho cá nhân, thường có tính phí.

ExpressVPN là một dịch vụ VPN như vậy vì nó đáp ứng trực tiếp nhu cầu riêng tư của khách hàng.

1.2.4.2 VPN doanh nghiệp

VPN doanh nghiệp, còn gọi là VPN doanh nghiệp, cho phép nhân viên từ xa của tổ chức kết nối an toàn với Internet như thể họ đang có mặt trực tiếp tại văn phòng.

Tuy nhiên, không giống như VPN thương mại, VPN doanh nghiệp có mục đích bảo vệ quyền riêng tư của công ty chứ không nhất thiết là của cá nhân.

1.2.4.3 Tự thiết lập VPN

Một số chuyên gia công nghệ và người đam mê tự làm chọn cách thiết lập VPN riêng bằng thiết bị của họ.

Tuy nhiên, VPN tự thiết lập không cung cấp khả năng bảo vệ các địa chỉ IP được chia sẻ, vị trí máy chủ ở nhiều quốc gia hoặc nhiều tính năng khác mà người dùng VPN thương mại được hưởng.

1.3 Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS...

Giao thức VPN là phương pháp mà thiết bị của bạn kết nối với máy chủ VPN. Một số giao thức tốt hơn về tốc độ , một số tốt hơn về bảo mật và một số chỉ hoạt động tốt hơn trong một số điều kiện mạng nhất định.

1.3.1 Giao thức đường hầm điểm-điểm PPTP (Point to Point Tunneling protocol)

1.3.1.1 Định nghĩa

Giao thức đường hầm điểm-điểm PPTP được đưa ra đầu tiên bởi một nhóm các công ty được gọi là PPTP Forum. Nhóm này bao gồm 3 công ty: Ascend comm., Microsoft, ECI Telematicsunication và US Robotic. Ý tưởng cơ sở của giao thức này là tách các chức năng chung và riêng của truy cập từ xa, lợi dụng cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa người dùng ở xa (client) và mạng riêng. Người dùng ở xa chỉ việc quay số tới nhà cung cấp dịch vụ Internet địa phương là có thể tạo đường hầm bảo mật tới mạng riêng của họ.

Giao thức PPTP được xây dựng dựa trên chức năng của PPP, cung cấp khả năng quay số truy cập tạo ra một đường hầm bảo mật thông qua Internet đến site đích. PPTP sử dụng giao thức bọc gói định tuyến chung GRE (Generic Routing Encapsulation) được mô tả lại để đóng gói và tách gói PPP, giao thức này cho phép PPTP mềm dẻo xử lý các giao thức khác không phải IP như: IPX, NETBEUI. Do PPTP dựa trên PPP nên nó cũng sử dụng PAP, CHAP để xác thực.

PPTP có thể sử dụng PPP để mã hoá dữ liệu nhưng Microsoft đã đưa ra phương thức mã hoá khác mạnh hơn đó là mã hoá điểm - điểm MPPE (Microsoft Point- to- Point Encryption) để sử dụng cho PPTP. Một ưu điểm của PPTP là được thiết kế để hoạt động ở lớp 2 (lớp liên kết dữ liệu) trong khi IPSec chạy ở lớp 3 của mô hình OSI. Bằng cách hỗ trợ việc truyền dữ liệu ở lớp thứ 2, PPTP có thể truyền trong đường hầm bằng các giao thức khác IP trong khi IPSec chỉ có thể truyền các gói IP

1.3.1.2 Cấu trúc của gói PPTP

Tiêu đề liên kết dữ liệu	Tiêu đề IP	Tiêu đề GRE	Tiêu đề PPP	Tải PPP được mã hoá (IP, IPX, NETBEUI)	Phần đuôi liên kết dữ liệu
--------------------------	------------	-------------	-------------	--	----------------------------

Đóng gói khung PPP. Phần tải PPP ban đầu được mật mã và đóng gói với phần tiêu đề PPP để tạo ra khung PPP. Sau đó, khung PPP được đóng gói với phần tiêu đề của phiên bản sửa đổi giao thức GRE. Đối với PPTP, phần tiêu đề của GRE được sửa đổi một số điểm sau:

- Một bit xác nhận được sử dụng để khẳng định sự có mặt của trường xác nhận 32 bit.
- Trường Key được thay thế bằng trường độ dài Payload 16bit và trường nhận dạng cuộc gọi 16 bit. Trường nhận dạng cuộc gọi Call ID được thiết lập bởi PPTP client trong quá trình khởi tạo đường hầm PPTP.
- Một trường xác nhận dài 32 bit được thêm vào. GRE là giao thức cung cấp cơ chế chung cho phép đóng gói dữ liệu để gửi qua mạng IP.

Đóng gói các gói GRE Tiếp đó, phần tải PPP đã được mã hoá và phần tiêu đề GRE được đóng gói với một tiêu đề IP chứa thông tin địa chỉ nguồn và đích cho PPTP client và PPTP server.

- Đóng gói lớp liên kết dữ liệu Do đường hầm của PPTP hoạt động ở lớp 2 - Lớp liên kết dữ liệu trong mô hình OSI nên lược đồ dữ liệu IP sẽ được đóng gói với phần tiêu đề (Header) và phần kết thúc (Trailer) của lớp liên kết dữ liệu.

Ví dụ, Nếu IP datagram được gửi qua giao diện Ethernet thì sẽ được đóng gói với phần Header và Trailer Ethernet. Nếu IP datagram được gửi thông qua đường truyền WAN điểm tới điểm thì sẽ được đóng gói với phần Header và Trailer của giao thức PPP.

1.3.2 Giao thức định hướng lớp 2 – L2F (Layer 2 Forwarding)

1.3.2.1 Định nghĩa

Giao thức định hướng lớp 2 L2F do Cisco phát triển độc lập và được phát triển dựa trên giao thức PPP (Point-to-Point Protocol). L2F cung cấp giải pháp cho dịch vụ quay số ảo bằng cách thiết lập một đường hầm bảo mật thông qua cơ sở hạ tầng công cộng như Internet. L2F là giao thức được phát triển sớm nhất, là phương pháp truyền thống để cho những người sử dụng ở xa truy cập vào một mạng công ty thông qua thiết bị truy cập từ xa. L2F cho phép đóng gói các gói PPP trong L2F, định đường hầm ở lớp liên kết dữ liệu.

1.3.2.2 Cấu trúc của gói L2F

1bit	1bit	1bit	1bit	8bit	1bit	3bit	8bit	8bit
F	K	P	S	Reserved	C	Version	Protocol	Sequence
Multiplex ID							Client ID	
Length							Offset	
Key								
Data								
Cchecksums								

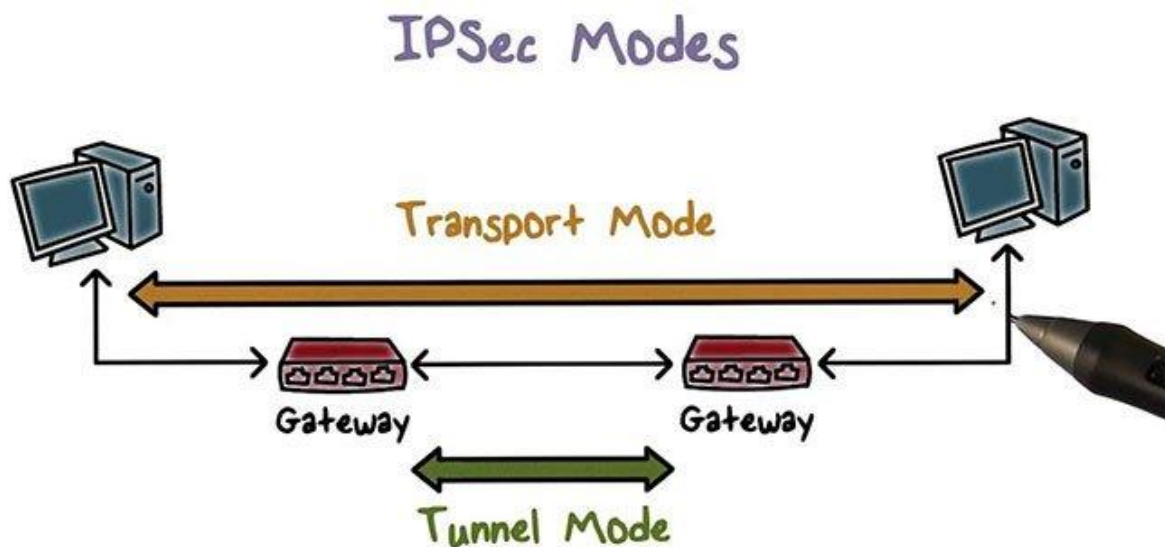
Trong đó:

- F: Trường “Offset” có mặt nếu bit này được thiết lập.
- K: Trường “Key” có mặt nếu bit này được thiết lập.
- P (Priority): Gói này là một gói ưu tiên nếu bit này được thiết lập
- S: Trường “Sequence” có mặt nếu bit này được thiết lập
- Reserved: luôn được đặt là 00000000
- Version: Phiên bản chính của L2F dùng để tạo gói. 3 bit luôn là 111
- Protocol: Xác định giao thức đóng gói L2F
- Sequence: Số chuỗi được đưa ra nếu trong L2F Header bit S=1
- Multiplex ID: nhận dạng một kết nối riêng trong một đường hầm (tunnel)
- Client ID: Giúp tách đường hầm tại những điểm cuối
- Length: chiều dài của gói (tính bằng byte) không bao gồm phần checksum

- Offset: Xác định số byte trước L2F header, tại đó dữ liệu tải tin được bắt đầu. Trường này có khi bit F=1
- Key: Trường này được trình bày nếu bit K được thiết lập. Đây là một phần của quá trình nhận xác thực
- Checksum: Kiểm tra tổng của gói. Trường checksum có nếu bit C=1

1.4 Các giao thức bảo mật cho VPN: IPSec, SSL/TLS.

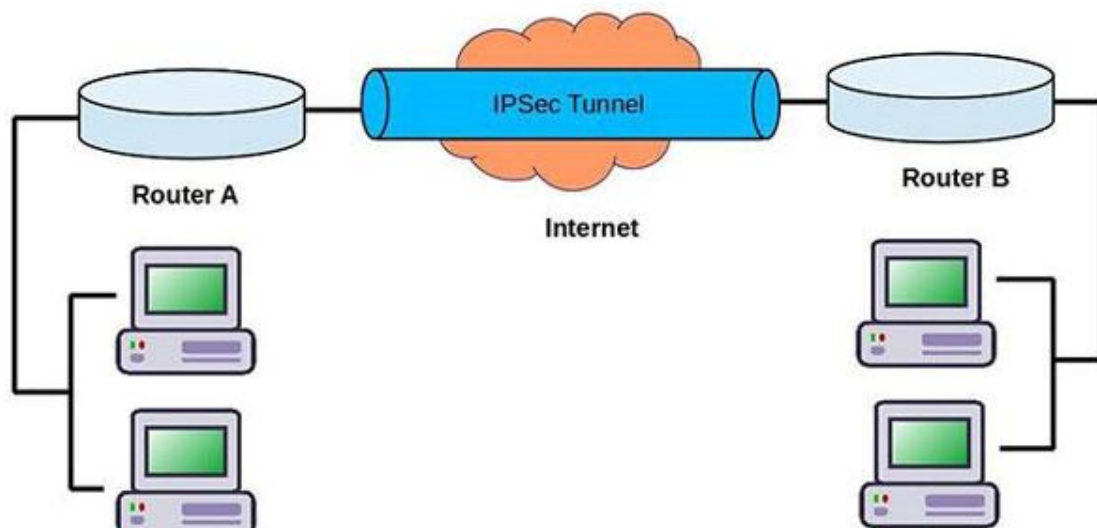
1.4.1 IPSec là gì?



IPSec (Internet Protocol Security – bảo mật mạng IP) là một bộ giao thức mật mã tiêu chuẩn bảo vệ lưu lượng dữ liệu qua mạng Internet Protocol (IP) được quy định bởi IETF (Internet Engineering Task Force - Nhóm đặc trách kỹ thuật Internet).

IPSec cung cấp xác thực (authentication), tính toàn vẹn (integrity) và tính bảo mật (confidentiality) cho kết nối qua mạng IP giữa 2 điểm liên lạc. Nó cũng chứa định nghĩa các gói mã hóa, giải mã, xác thực và các giao thức cần thiết để trao đổi khóa an toàn và quản lý khóa.

1.4.1.1 Công dụng của IPSec



IPSec có thể được sử dụng cho các công việc như:

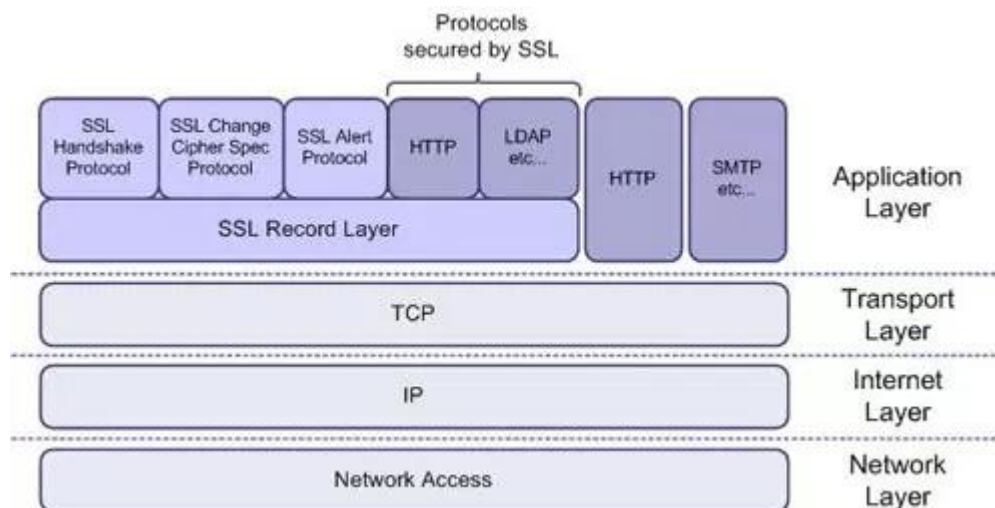
- Mã hóa dữ liệu lớp ứng dụng.
- Cung cấp bảo mật cho các bộ định tuyến gửi dữ liệu định tuyến qua internet công cộng.
- Cung cấp xác thực không mã hóa, như xác thực rằng dữ liệu bắt nguồn từ một người gửi đã biết.
- Bảo vệ dữ liệu mạng bằng cách thiết lập các mạch sử dụng đường hầm IPsec, trong đó tất cả dữ liệu đang được gửi giữa hai điểm cuối được mã hóa, như với kết nối Mạng riêng ảo (VPN).

1.4.2 Giao thức SSL/TLS

1.4.2.1 Giao thức TLS là gì

- Tiêu chuẩn TLS - transport layer security hay còn gọi là giao thức bảo mật tầng giao vận. Giao thức này được phát triển dựa trên tiêu chuẩn SSL v3.0 (Secure Socket Layer)
- Giao thức TLS phiên bản v1.0 (TLS v1.0) do tổ chức Internet Engineering Task Force (IETF) công bố tại RFC 2246 tháng 01/1999.
- Tuy nói rằng giao thức TLS v1.0 được phát triển dựa trên giao thức SSL v3.0 nhưng chúng cũng có những điểm khác biệt mà trong đó điểm khác biệt lớn nhất chính là sự không tương thích giữa chúng.

1.4.2.2 Cấu trúc của giao thức SSL



- Do giao thức TLS được phát triển dựa trên giao thức SSL nên chúng ta cùng tìm hiểu một chút về cấu trúc của giao thức SSL trước nhé. Chúng ta cùng xem hình minh họa.
- Theo hình minh họa trên thì cấu trúc và giao thức SSL được đặt giữa tầng vận chuyển (Transport Layer) và tầng ứng dụng (Application Layer)
- Giao thức SSL cung cấp giao thức bảo mật truyền thông có 3 đặc điểm nổi bật:
 - Các bên giao tiếp (nghĩa là client và server) có thể xác thực nhau bằng cách sử dụng mật mã khóa chung

- Sự bí mật của lưu lượng dữ liệu được bảo vệ vì nối kết được mã hóa trong suốt sau khi một sự thiết lập quan hệ ban đầu và sự thương lượng khóa session đã xảy ra.
- Tính xác thực và tính toàn vẹn của lưu lượng dữ liệu cũng được bảo vệ vì các thông báo được xác thực và được kiểm tra tính toàn vẹn một cách trong suốt bằng cách sử dụng MAC.

1.5 Tìm hiểu về SoftEther VPN

1.5.1 SoftEther VPN là gì?

Softether là một dự án VPN tương đối mới giúp công nghệ VPN trở nên an toàn hơn, cho phép người dùng lướt web ẩn danh và BẢO MẬT cao hơn. SoftEther là một trong những đa giao thức mạnh mẽ và dễ sử dụng nhất trên thế giới.

- SoftEther VPN hỗ trợ Windows, Linux, Mac, Solaris, FreeBSD và thường là một lựa chọn tốt để thay thế cho OpenVPN vì nhanh hơn. SoftEther VPN cũng hỗ trợ Microsoft SSTP VPN cho Windows Vista/7/8.
- Bên cạnh ưu điểm nhanh, SoftEther VPN còn sử dụng key certificate AES 256 bit,, 1 cấp độ bảo mật và mã hóa cao. Thêm một điểm cộng lớn cho phần mềm này là nó tích hợp tất cả các tính năng của các giao thức VPN khác nhau như PPTP, L2TP, OpenVPN và SSTP, trong khi loại bỏ nhược điểm của chúng.
- Tất cả các tính năng mà SoftEther cung cấp, tăng cường khả năng giúp người dùng điều hướng an toàn và vượt qua mọi tường lửa do các bên chính quyền áp đặt, giúp nó trở thành một giao thức VPN phổ biến.

1.5.1.1 SoftEther VPN – Thông số kỹ thuật chi tiết

- Có sẵn theo giấy phép GNU GPL;
- SoftEther VPN hỗ trợ chứng chỉ xác thực RSA và tính năng Deep Inspect Packet Logging;
- Hỗ trợ các giao thức OpenVPN, EtherIP, L2TP và Microsoft SSTP;
- Hỗ trợ IPV6, Packet Filtering và tính năng DNS động;
- Sử dụng mã hóa AES 256-bit;
- SoftEther VPN tuân thủ Virtual Network Adapter, trong khi máy chủ SoftEther VPN tuân thủ Virtual Ethernet Switch;
- Nhúng dynamic-DNS và NAT-traversal;
- Chạy trên Windows, Linux, FreeBSD, Solaris, iOS, Android và Mac OS;
- SoftEther VPN Protocol hỗ trợ đa ngôn ngữ (tiếng Anh, tiếng Nhật và tiếng Trung).

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

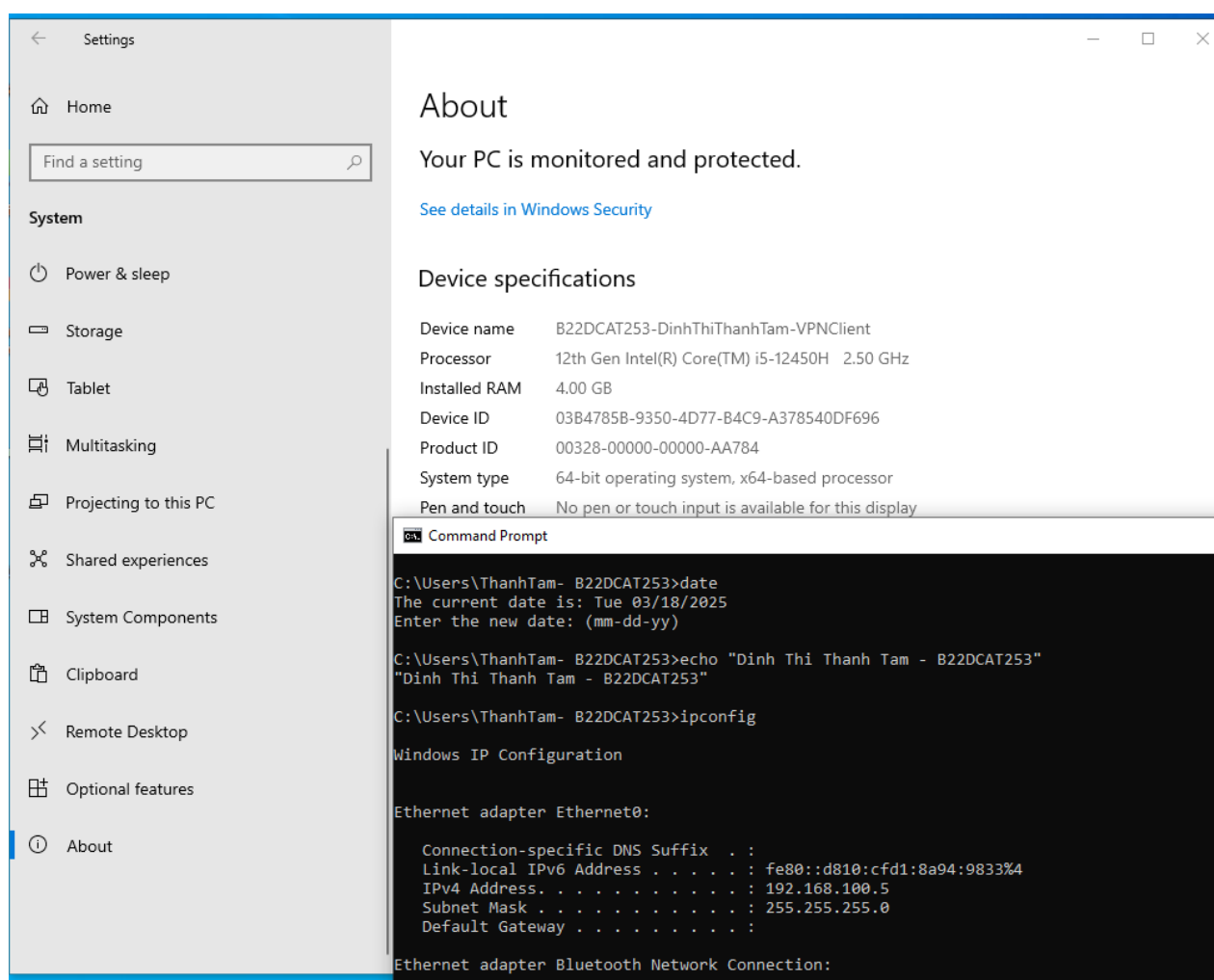
2.1 Chuẩn bị môi trường

- 01 máy tính chạy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng (LAN hoặc Internet) để cài đặt VPN server.
- 01 máy tính chạy MS Windows để cài đặt VPN client

2.2 Các bước thực hiện

2.2.1 Chuẩn bị hệ thống

- Máy Windows đặt tên: <Mã SV-Tên SV>-VPNClient



- Máy Linux (VPN Server) đặt tên: <Mã SV-Tên SV>-VPNServer

```
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~
File Actions Edit View Help
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ date
Thu Mar 20 10:49:35 AM EDT 2025

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ hostnamectl

Static hostname: b22dcat253-DinhThiThanhTam-VPNServer
Icon name: computer-vm
```

- Cấu hình địa chỉ IP và đảm bảo kết nối mạng LAN.

2.2.2 Cài đặt SoftEther VPN Server trên Linux

Tải SoftEther VPN Server tại: <https://www.softether.org/5-download>

```
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~
File Actions Edit View Help
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ wget https://www.softether-download.com/files/softether/v4.41-9787-rtm-2023.03.14-tree/Linux/SoftEther_VPN_Server/64bit_-Intel_x64_or_AMD64/softether-vpnserver-v4.41-9787-rtm-2023.03.14-linux-x64-64bit.tar.gz
--2025-03-20 10:53:54-- https://www.softether-download.com/files/softether/v4.41-9787-rtm-2023.03.14-tree/Linux/SoftEther_VPN_Server/64bit_-Intel_x64_or_AMD64/softether-vpnserver-v4.41-9787-rtm-2023.03.14-linux-x64-64bit.tar.gz
Resolving www.softether-download.com (www.softether-download.com)... 130.158.75.49
Connecting to www.softether-download.com (www.softether-download.com)|130.158.75.49|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8399149 (8.0M) [application/x-gzip]
Saving to: 'softether-vpnserver-v4.41-9787-rtm-2023.03.14-linux-x64-64bit.tar.gz'

softether-vpnserver 100%[=====>] 8.01M 690KB/s in 13s

2025-03-20 10:54:08 (619 KB/s) - 'softether-vpnserver-v4.41-9787-rtm-2023.03.14-linux-x64-64bit.tar.gz' saved [8399149/8399149]
```

2.2.2.1 Giải nén & cài đặt:

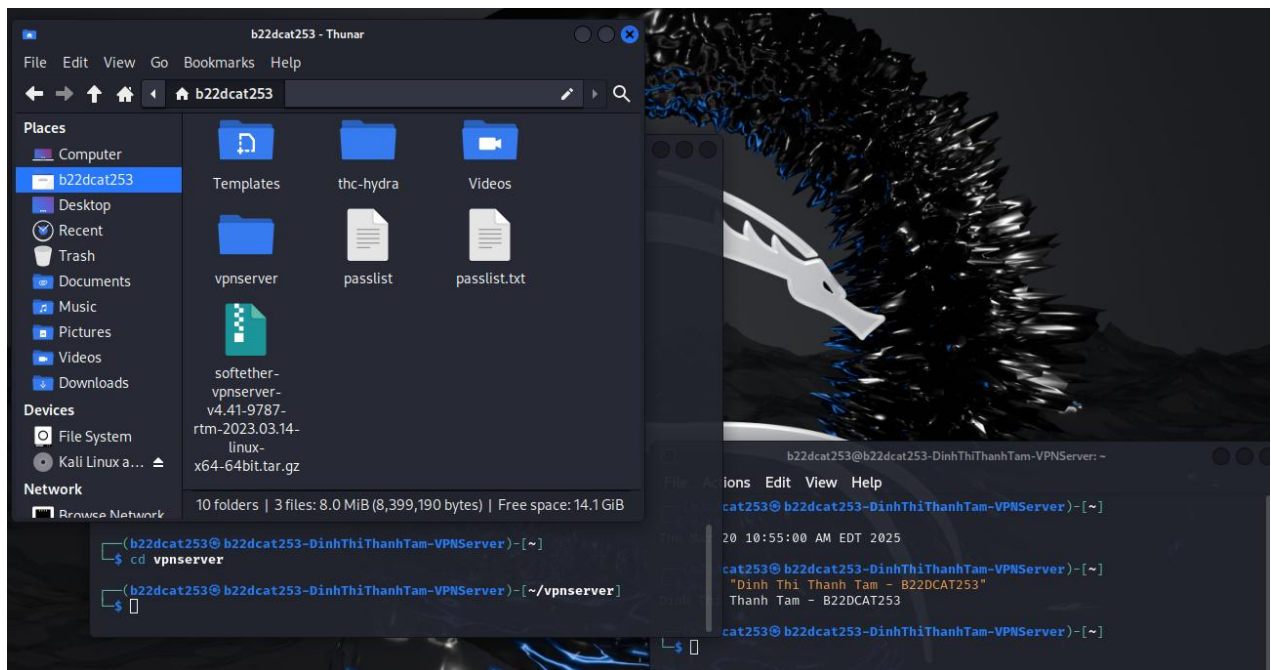
Cài đặt và cấu hình VPN Server theo hướng dẫn sau:

- Giải nén file cài đặt bằng lệnh
tar -vxzf <tên file vpn server>

```
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~
File Actions Edit View Help
$ tar -vxzf softether-vpnserver-v4.41-9787-rtm-2023.03.14-linux-x64-64bit.tar.gz
vpnserver/
vpnserver/Makefile
vpnserver/.install.sh
vpnserver/ReadMeFirst_License.txt
vpnserver/Authors.txt
vpnserver/ReadMeFirst_Important_Notices_ja.txt
vpnserver/ReadMeFirst_Important_Notices_en.txt
vpnserver/ReadMeFirst_Important_Notices_cn.txt
vpnserver/code/
```

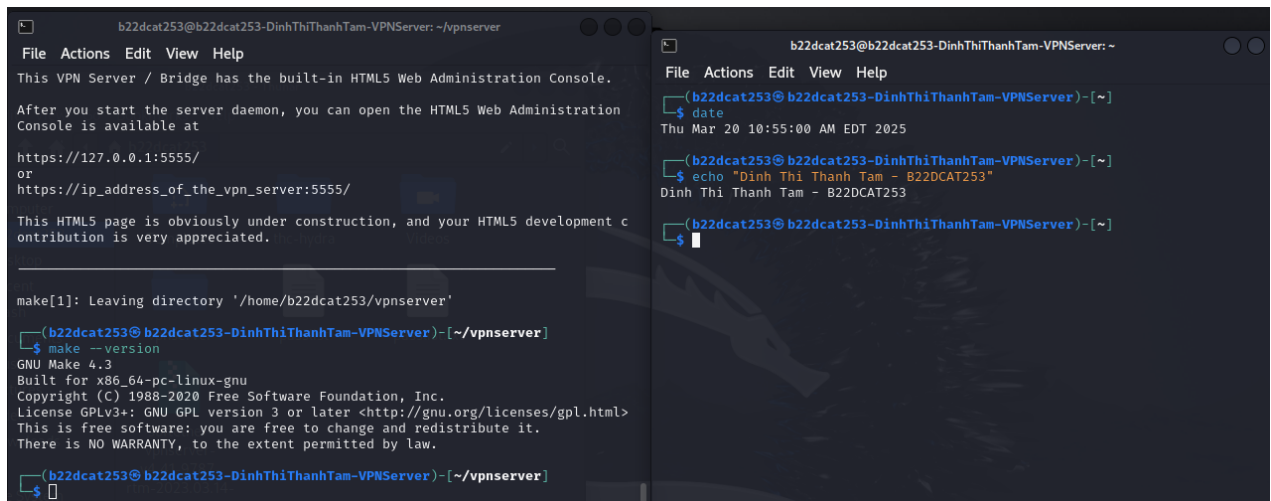
- Chuyển vào thư mục VPN server

cd vpnserver



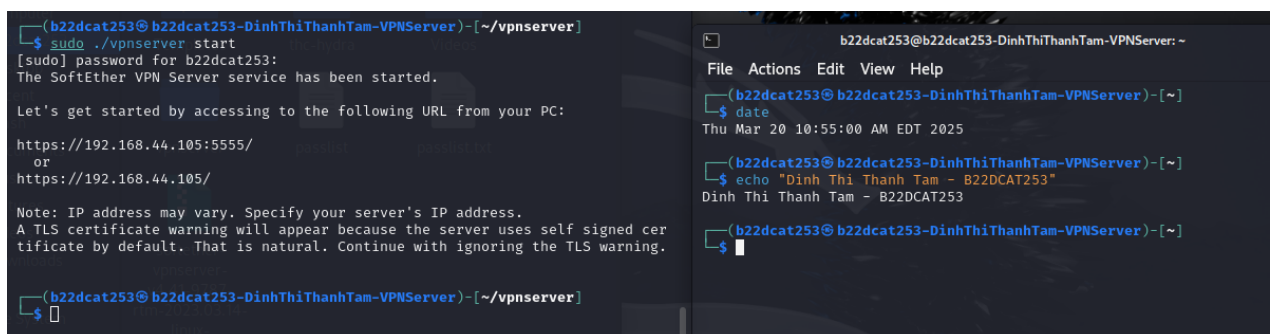
- Biên dịch và cài đặt:

make # Hệ thống cần có gcc



- Khởi động máy chủ VPN

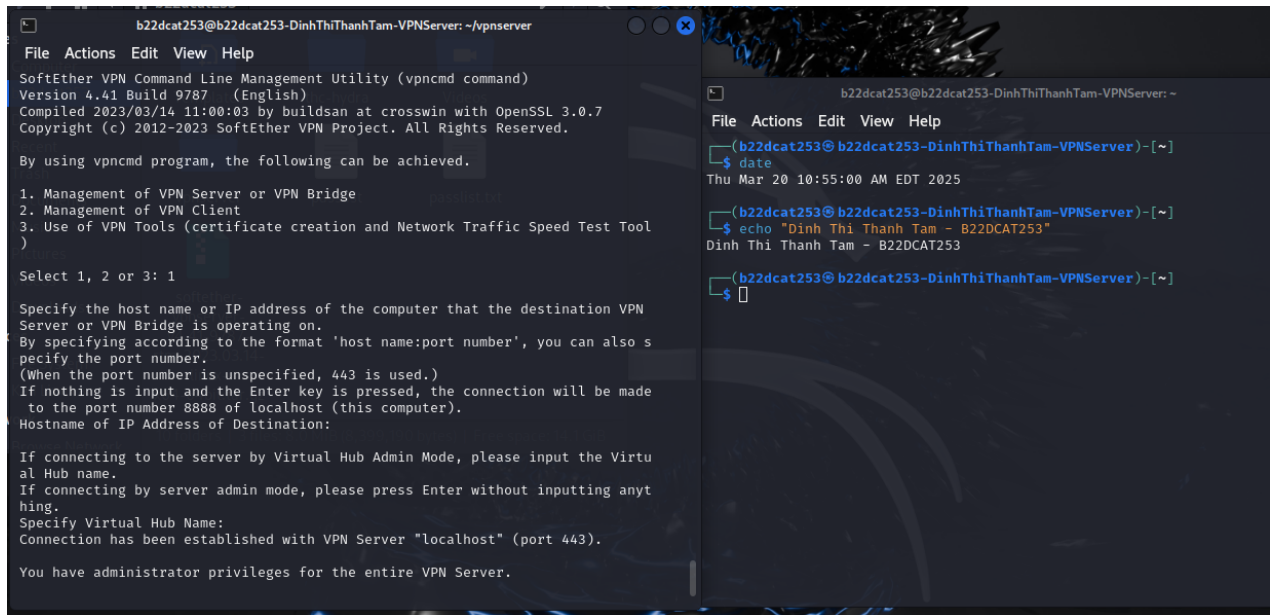
sudo ./vpnservice start



- Chạy tiện ích quản trị viên VPN Server Manager:

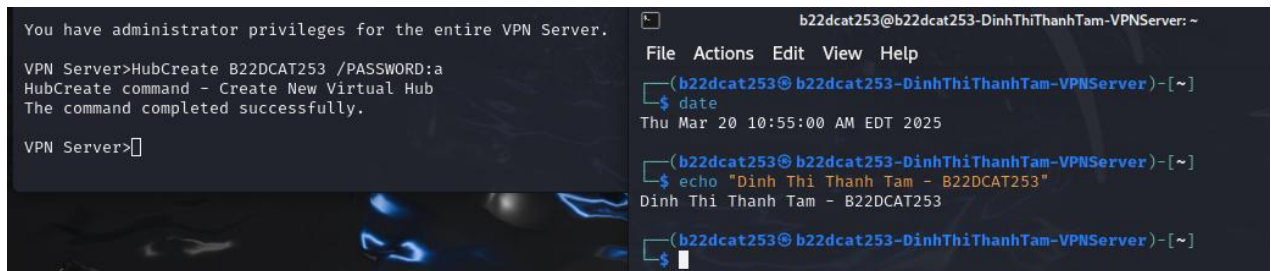
./vpncmd

- Chọn chức năng số 1 → Nhấn Enter 2 lần.



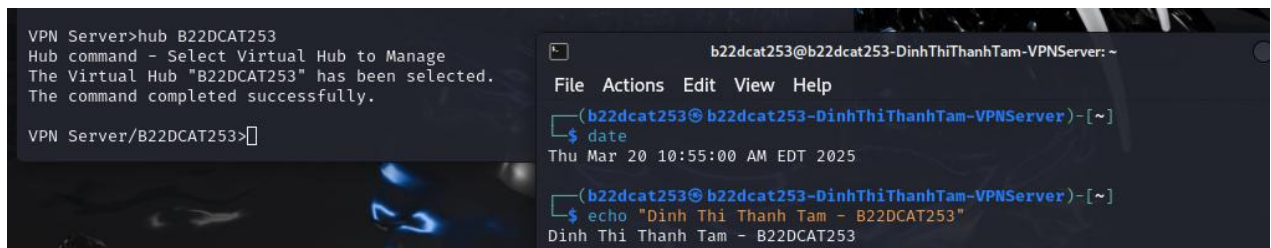
2.2.2.2 Tạo Virtual Hub & tài khoản VPN

HubCreate <Tên Virtual Hub: MSV> /PASSWORD:<mật khẩu>



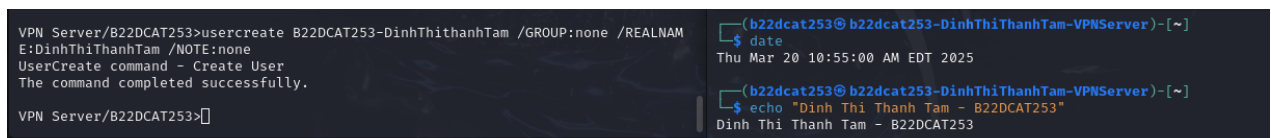
- Chọn Virtual Hub đã tạo

Hub <MSV>



- Tạo 1 người dùng VPN mới:

UserCreate <mã sv-tên> /GROUP:none /REALNAME:Tên SV /NOTE:none



- Đặt mật khẩu cho người dùng:

UserPasswordSet <mã sv-tên> /PASSWORD:<mật khẩu>

```
VPN Server/B22DCAT253>Userpasswordset B22DCAT253-DinhThiThanhTam /PASSWORD:a
UserPasswordSet command - Set Password Authentication for User Auth Type and Set
Password
The command completed successfully.
VPN Server/B22DCAT253>

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer) - [~]
$ date
Thu Mar 20 10:55:00 AM EDT 2025
(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer) - [~]
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253
```

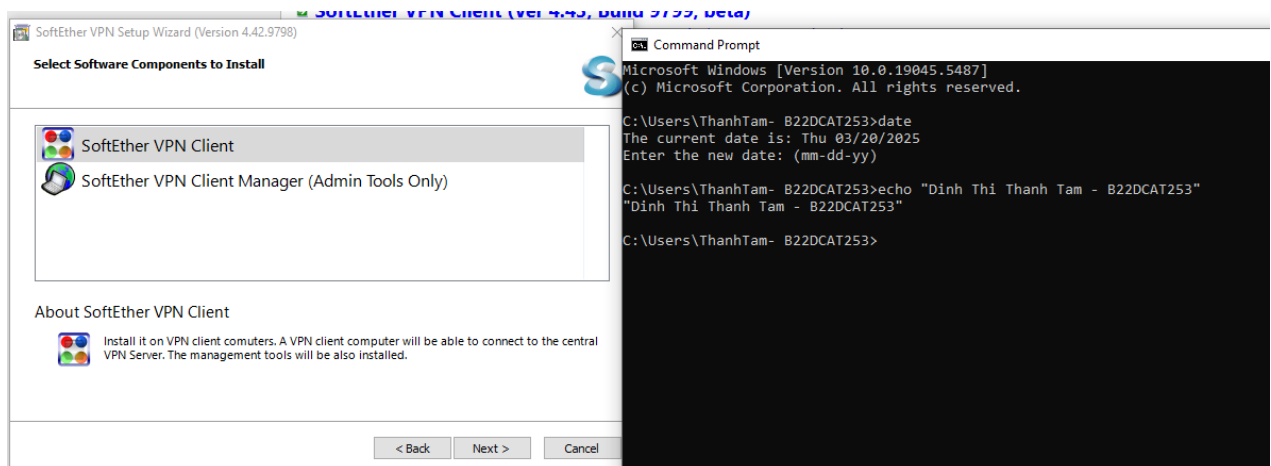
- Thoát khỏi quản trị: *exit*

```
VPN Server/B22DCAT253>exit

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer) - [~/vpnservice]
$
```

2.2.3 Cài đặt SoftEther VPN Client trên Windows

- Tải từ: <https://www.softether.org/5-download>

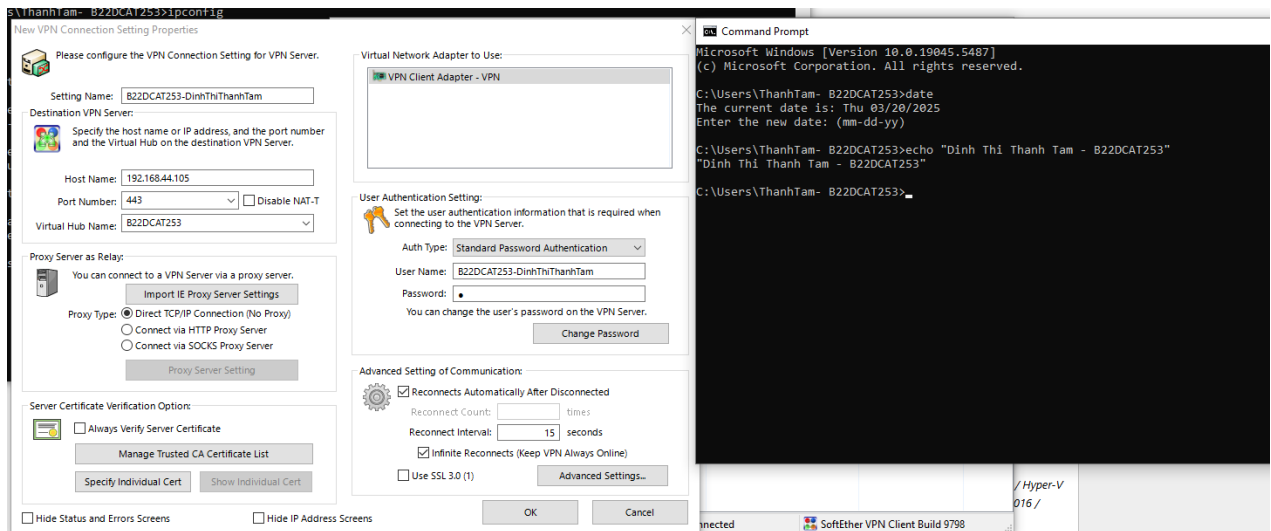


- Cài đặt và mở SoftEther VPN Client Manager.

2.2.4 Tạo & kiểm tra kết nối VPN

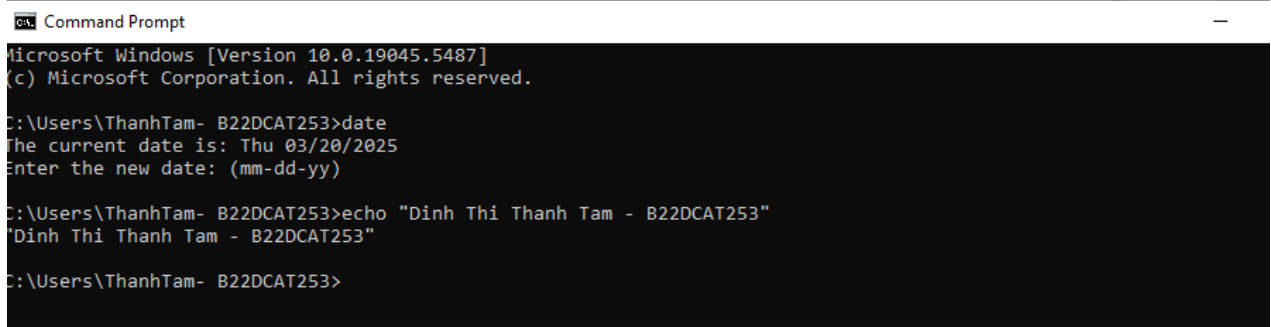
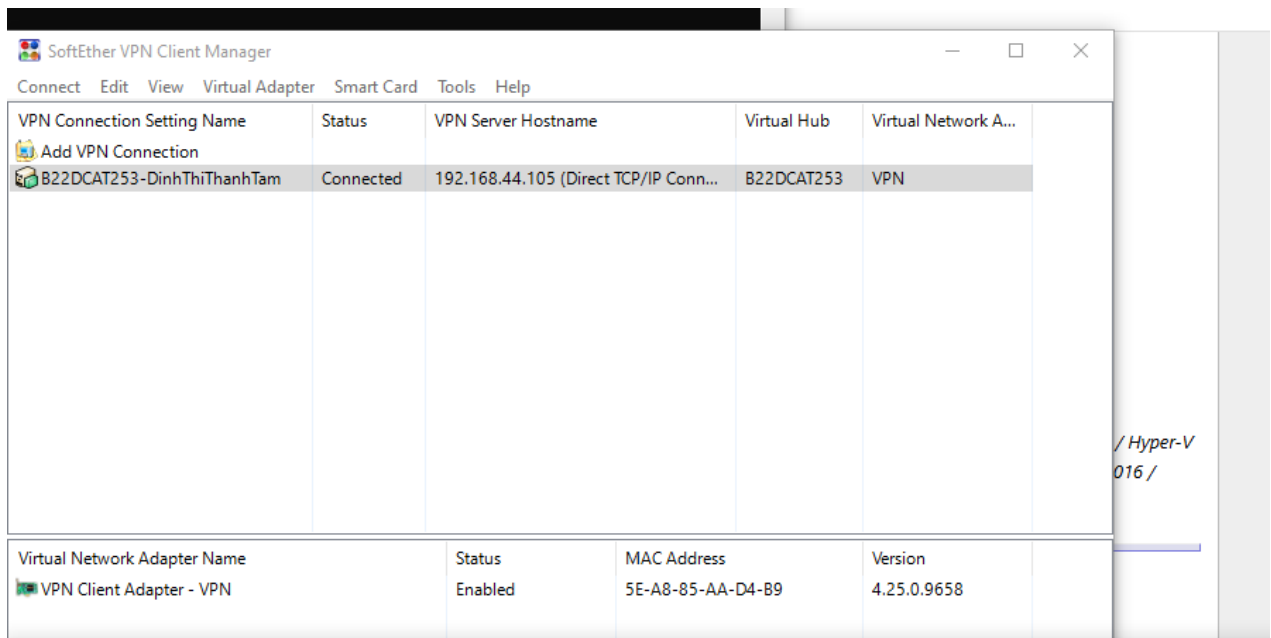
2.2.4.1 Trong SoftEther VPN Client Manager, thêm kết nối mới với:

- Địa chỉ IP máy chủ VPN: 192.168.44.105
- Tên Virtual Hub: B22DCAT253-DinhThithanhTam
- Tên người dùng và mật khẩu: B22DCAT253
- Đặt tên kết nối: <Mã SV>-<Họ tên>: B22DCAT253-DinhThiThanhTam



2.2.4.2 Thử kết nối VPN:

- Nếu thành công, trạng thái sẽ báo Connected.



2.2.4.3 Kiểm tra log trên VPN Server:

- Chuyển sang máy chủ VPN, mở 1 terminal mới chuyển đến thư mục vpnserver/server_log để kiểm tra log trên VPN server:

```
(root@ b22dcat253-DinhThiThanhTam-VPNServer)-[/home/b22dcat253/vpnserver]
# cd server_log

(root@ b22dcat253-DinhThiThanhTam-VPNServer)-[/home/b22dcat253/vpnserver/server_log]
#
```

sudo grep <mã sinh viên> vpnserver/server_log/.log*

```
root@b22dcat253-DinhThiThanhTam-VPNServer: /home/b22dcat253/vpnserver/server_log
File Actions Edit View Help

(root@ b22dcat253-DinhThiThanhTam-VPNServer)-[/home/b22dcat253/vpnserver/server_log]
# grep B22DCAT253 *.log
2025-03-20 11:13:45.443 Administration mode [RPC-27]: A new Virtual Hub "B22DCAT253" has been created.
2025-03-20 11:13:45.443 Virtual Hub "B22DCAT253" has been started.
2025-03-20 11:13:45.443 The MAC address of Virtual Hub "B22DCAT253" is "00-AE-19-3A-67-2C".
2025-03-20 11:13:45.443 [HUB "B22DCAT253"] The Virtual Hub is now online.
2025-03-20 11:19:37.571 [HUB "B22DCAT253"] Administration mode [RPC-30] (Virtual Hub "B22DCAT253"): User "B22DCAT253-DinhThiThanhTam" has been created.
2025-03-20 11:23:26.063 [HUB "B22DCAT253"] Administration mode [RPC-30] (Virtual Hub "B22DCAT253"): The setting of user "B22DCAT253-DinhThiThanhTam" has been updated.
2025-03-20 11:54:09.985 [HUB "B22DCAT253"] The connection "CID-4" (IP address: 192.168.44.100, Host name: 192.168.44.100, Port number: 52456, Client name: "SoftEther VPN Client", Version: 4.42, Build: 9798) is attempting to connect to the Virtual Hub. The auth type provided is "Password authentication" and the user name is "B22DCAT253-DinhThiThanhTam".
2025-03-20 11:54:09.985 [HUB "B22DCAT253"] Connection "CID-4": Successfully authenticated as user "B22DCAT253-DinhThiThanhTam".
2025-03-20 11:54:09.985 [HUB "B22DCAT253"] Connection "CID-4": The new session "SID-B22DCAT253-DINHITHITHANHHTAM-1" has been created. (IP address: 192.168.44.100, Port number: 52456, Physical underlying protocol: "Standard TCP/IP (IPv4)")
2025-03-20 11:54:09.985 [HUB "B22DCAT253"] Session "SID-B22DCAT253-DINHITHITHANHHTAM-1": The parameter has been set. Max number of TCP connections: 2, Use of encryption: Yes, Use of compression: No, Use of Half duplex communication: No, Timeout: 20 seconds.
2025-03-20 11:54:09.996 [HUB "B22DCAT253"] Session "SID-B22DCAT253-DINHITHITHANHHTAM-1": VPN Client details: (Client product name: "SoftEther VPN Client", Client version: 442, Client build number: 9798, Server product name: "SoftEther VPN Server (64 bit)", Server version: 441, Server build number: 9787, Client OS name: "Windows 10", Client OS version: "Build 19045, Multiprocessor Free (19041.vb_release.191206-1406)", Client product ID: "--", Client host name: "B22DCAT253-DinhThiThanhTam-VPNClient", Client IP address: "192.168.197.129", Client port number: 49974, Server host name: "192.168.44.105", Server IP address: "192.168.44.105", Server port number: 443, Proxy host name: "", Proxy IP address: "0.0.0.0", Proxy port number: 0, Virtual Hub name: "B22DCAT253", Client unique ID: "6760404F312364B0D66C3325B5EF8064")

(root@ b22dcat253-DinhThiThanhTam-VPNServer)-[/home/b22dcat253/vpnserver/server_log]
# date
Thu Mar 20 12:04:44 PM EDT 2025

(root@ b22dcat253-DinhThiThanhTam-VPNServer)-[/home/b22dcat253/vpnserver/server_log]
# echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253

(root@ b22dcat253-DinhThiThanhTam-VPNServer)-[/home/b22dcat253/vpnserver/server_log]
#
```

➔ Kết nối thành công, log hiển thị các dòng liên quan đến <mã sinh viên> :
B22DCAT253

KẾT LUẬN

Qua bài thực hành này, cung cấp kiến thức tổng quan về mạng riêng ảo (VPN) và các giao thức liên quan. Quá trình cài đặt, cấu hình và kiểm tra kết nối VPN đã giúp hiểu rõ hơn về cách triển khai một hệ thống VPN thực tế.

Cụ thể, bài thực hành đã hoàn thành các nội dung sau:

- Tìm hiểu về VPN: Hiểu được khái niệm, lợi ích, các giao thức đường hầm (PPTP, L2TP, L2F, MPLS) và giao thức bảo mật (IPSec, SSL/TLS).
- Cài đặt và cấu hình SoftEther VPN Server trên Linux: Bao gồm việc tải về, cài đặt, khởi động dịch vụ và tạo tài khoản VPN.
- Cài đặt SoftEther VPN Client trên Windows: Kết nối tới máy chủ VPN, xác thực thông tin đăng nhập và kiểm tra trạng thái kết nối.
- Kiểm tra và đánh giá kết quả: Xác nhận kết nối thành công giữa VPN Client và VPN Server thông qua kiểm tra log và trạng thái hệ thống.

Bài thực hành này không chỉ có kiến thức lý thuyết mà còn có kỹ năng thực hành trong việc thiết lập và quản trị hệ thống VPN, góp phần nâng cao hiểu biết về bảo mật mạng và ứng dụng trong thực tế.

TÀI LIỆU THAM KHẢO

- [1] <https://vncoder.vn/tin-tuc/cong-nghe/tong-quan-ve-vpn>
- [2] <https://br.atsit.in/vi/?p=54681>
- [3] <https://www.hocviendaotao.com/2013/03/giao-thuc-ipsec.html>
- [4] <https://datatracker.ietf.org/doc/html/rfc8446>
- [5] <https://www.softether.org/4-docs>